REMARKS

Applicants submit the present Amendment to address the issues raised in the Office Action mailed December 20, 2006. The Office Action states that pending Claims 1-22 stand rejected under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 7,073,198 to Flowers et al. ("Flowers") in view of U.S. Patent Application Publication No. 2004/0006704 to Dahlstrom et al. ("Dahlstrom"). For the reasons discussed below, Applicants respectfully submit that the pending claims are patentable over the cited art, and request that a Notice of Allowance therefore be issued in due course.

I. The Claim Amendments

Applicants have amended Claim 5 to depend from Claim 4, Claim 8 to depend from Claim 2, Claim 15 to depend from Claim 14 and Claim 18 to depend from Claim 12. No other amendments have been made to the claims.

II. The Rejections of Claims 1, 11 and 21

Independent Claims 1, 11 and 21 stand rejected under 35 U.S.C. § 103(a) as being obvious over Flowers in view of Dahlstrom. Independent Claim 1 recites:

> 1. A method of administering a countermeasure for a computer security threat to a computer system, comprising:
>
> establishing a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);
>
> receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and
>
> processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

Claims 11 and 21 are corresponding system and computer program product claims, respectively. Applicants respectfully traverse the rejections of Claims 1, 11 and 21 for at least the following two independent reasons.

First, the Office Action cites to paragraph [0006] of Dahlstrom as disclosing the second recitation of Claim 1. (Office Action at 3). This paragraph of Dahlstrom recites:

> In one embodiment of the present invention, a method for determining security vulnerabilities is disclosed that includes **receiving a profile of one or more products used by an organization, the profile including characteristics of each product**. The method further includes comparing the characteristics of each product to a plurality of product records, each product record including one or more security vulnerabilities associated with the product record and one or more fixes associated with each security vulnerability. The method further includes determining at least one security vulnerability of the one or more security vulnerabilities for at least one of the one or more products in response to comparing the characteristics of the at least one of the one or more products to the product record.

Thus, Dahlstrom teaches "receiving a profile of one or more products used by an organization" where the profile lists characteristics of each product used by the organization. In contrast, Claims 1, 11 and 21 recite "receiving a [Threat Management Vector]" or "TMV", where the TMV contains (1) a field that identifies an operating system that is affected by a computer security threat, (2) a field that identifies an operating system release level and (3) a field that identifies a set of possible countermeasures for the identified operating system/release level. Applicants respectfully submit that the "organization profile" discussed in paragraph 0006 of Dahlstrom does not teach or suggest the Threat Management Vector of Claims 1, 11 and 21.

Paragraph 0006 of Dahlstrom also discusses a "plurality of product records", where each such record includes a security vulnerability and one or more fixes thereto. However, these product records are not "received" as recited in Claims 1, 11 and 21, but instead comprise part of a "security vulnerabilities database 50." (*See, e.g.*, Dahlstrom at ¶ 0024-0025). Thus, as neither of the cited references disclose "receiving a TMV" as recited in Claims 1, 11 and 21, the rejection of Claims 1, 11 and 21 under 35 U.S.C. § 103 should be withdrawn.

Applicants also respectfully submit that the rejections of Claims 1, 11 and 21 should be withdrawn because a person of ordinary skill in the art would not have been motivated to combine Flowers and Dahlstrom in the manner suggested in the pending rejections. Flowers is directed to a system for detecting the vulnerabilities of a network without subjecting the network to undue risk. (*See, e.g.,* Flowers at Col. 4, lines 14-20). In particular, the system of Flowers sends out several sets of packets to a remote host and, based on the response of the remote host to these sets of packets, determines the operating system, version and patch level of the remote host. (*See* Flowers at Col. 4, lines 26-55). In contrast, the system of Dahlstrom is directed to a securities vulnerability database 50 that may be compared to an organizational profile 72. The organization desiring a security review completes and submits an organizational profile 72 that lists the "computing, networking and telephony hardware and software products used by the organization." (Dahlstrom at ¶ 0036). The system of Dahlstrom then searches the securities vulnerability database 50 to identify vulnerabilities associated with the organizations products. (*Id.*). As should be clear from the above description, the system of Flowers is directed to determining the particular operating system, version and patch status of a particular remote device. In contrast, the system of Dahlstrom involves taking already known information regarding all of the hardware and software used by an organization, and searching a database to identify particular vulnerabilities associated with this known hardware and software. One of skill in the art would not have been motivated to incorporate the system of Dahlstrom into the system of Flowers as the system of Dahlstrom requires that an organization already provide a complete list of the organizations hardware and software products. Accordingly, this provides an independent basis for withdrawal of the rejections of Claims 1, 11 and 21.

III. The Rejections of Claims 2 and 12

Claims 2 and 12 likewise stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 3). As Claims 2 and 12 depend from Claims 1 and 11, respectively, the rejections of Claims 2 and 12 should be withdrawn for each of the reasons,

discussed above, that the rejections of Claims 1 and 11 should be withdrawn. In addition, Applicants respectfully submit that Claims 2 and 12 are independently patentable over the cited art. In particular, the Office Action relies on Dahlstrom as disclosing the recitations added by Claims 2 and 12, which recite, among other things, "receiving a TMV history file in response to installation, configuration or maintenance of the computer system." However, the cited portion of Dahlstrom (¶ 0018) simply does not disclose the recitation of Claims 2 or 12. The cited portion of Dahlstrom says nothing about receiving a TMV history file, let alone receiving such a file "in response to installation, configuration or maintenance of the computer system" as recited in Claims 2 and 12. In fact, it appears that paragraph 0018 of Dahlstrom was cited against Claims 2 and 12 because it includes the word "installation." As such, the rejections of Claims 2 and 12 should thus be withdrawn for at least this additional reason.

IV. The Rejections of Claims 3 and 13

Claims 3 and 13 likewise stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 3-4). As Claims 3 and 13 depend from Claims 1-2 and 11-12, respectively, the rejections of Claims 2 and 12 should be withdrawn for each of the reasons, discussed above, that the rejections of Claims 1-2 and 11-12 should be withdrawn. In addition, Applicants respectfully submit that Claims 3 and 13 are independently patentable over the cited art. In particular, the Office Action cites to paragraphs 0027 and 0036 of Dahlstrom as disclosing the recitations of Claims 3 and 13. However, the cited portions of Dahlstrom relate to the updating of the product records 52, which appears to be what the Office Action is alleging comprises the TMV of the pending claims. In contrast, what Claims 3 and 13 recite is "updating a threat management information base for the computer system to account for the countermeasures that are processed." The product records 52 are not a "threat management information base for the computer system" that is subject to a computer security threat (instead, they are part of a database of the system of Dahlstrom), nor does the "updating" discussed in paragraphs 0027 and 0036 of Dahlstrom have anything to do with "account[ing] for the

countermeasures that are processed" as recited in Claims 3 and 13. Accordingly, the rejections of Claims 3 and 13 should also be withdrawn for at least these additional reasons.

V. The Rejections of Claims 4, 14 and 22

Claims 4, 14 and 22 likewise stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 4). As Claims 4, 14 and 22 depend from Claims 1, 11 and 21, respectively, the rejections of Claims 4, 14 and 22 should be withdrawn for each of the reasons, discussed above, that the rejections of Claims 1, 11 and 21 should be withdrawn. In addition, Applicants respectfully submit that Claims 4, 14 and 22 are independently patentable over the cited art. In particular, the Office Action cites to Col. 4, lines 26-37 of Flowers as disclosing "adding at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat" as recited in Claims 4, 14 and 22. However, the cited portion of Flowers recites, in its entirety:

> A system and method in accordance with the invention reliably and non-intrusively identifies various conditions of a network. In particular, an embodiment of the invention can identify an operating system, including version and patch level, and a service, including version and patch level, of a remote host on the network. Using this information, an embodiment of the invention can then reliably identify a vulnerability condition of the network. In some embodiments, the operating system and service information can be used to identify a trojan application, unlicensed software use, security policy violations, or even infer vulnerabilities that are yet unknown.

(Flowers at Col. 4, lines 26-37). As is clear from a careful review of the above quote, the cited portion of Flowers has nothing to do with instance identifiers or accounting for multiple instances of an operating system running in the computer system as recited in Claims 4, 14 and 22. Accordingly, the rejections of Claims 4, 14 and 22 should also be withdrawn for at least these additional reasons.

VI. The Rejections of Claims 6 and 16

Claims 6 and 16 also stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 4-5). As Claims 6 and 16 depend from Claims 1 and 11, respectively, the rejections of Claims 6 and 16 should be withdrawn for each of the reasons, discussed above, that the rejections of Claims 1 and 11 should be withdrawn. In addition, Applicants respectfully submit that Claims 6 and 16 are independently patentable over the cited art.

The Office Action once again cites to Col. 4, lines 26-37 of Flowers, which is quoted immediately above, as disclosing the first recitation of Claims 6 and 16. However, the cited portion of Flowers simply does not disclose including a fourth field in a TMV that identifies at least one application program type or a fifth field the identifies a release level for the application program type along with the information of the first through third fields recited in the TMV of Claims 6 and 16. Thus, it is clear that the Office Action is taking the position that the **product records 52** of Dahlstrom should be combined with the **results** provided by the system of Flowers (i.e., the identification of the operating system, including version and patch level, discussed at Col. 4, lines 26-37 of Flowers) to allegedly arrive at a TMV according to embodiments of the present invention. Applicants respectfully submit that this combination does not make any sense, and that no motivation for such a combination can be found in either the cited references or the prior art in general. In fact, the only motivation for such a combination is using the present invention as a road map. However, the teachings of the present invention cannot properly be used as motivation for a combination under Section 103. Accordingly, the rejections of Claims 6 and 16 should be withdrawn for this additional reason.

VII. The Rejections of Claims 7 and 17

Claims 7 and 17 also stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 5). As Claims 7 and 17 depend from Claims 1 and 6 and Claims 11 and 16, respectively, the rejections of Claims 7 and 17 should be withdrawn for each of the

reasons, discussed above, that the rejections of Claims 1 and 6 and Claims 11 and 16, respectively, should be withdrawn. In addition, Claims 7 and 17 include the same recitation of Claims 4 and 14, discussed above, that is not found in the cited art. Accordingly, the rejections of Claims 7 and 17 should also be withdrawn for the same reasons, discussed above, that the rejections of Claims 4 and 14 should be withdrawn.

VIII. The Rejections of Claims 9 and 19

Claims 9 and 19 also stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 5). As Claims 9 and 19 depend from Claims 1 and 11, respectively, the rejections of Claims 9 and 19 should be withdrawn for each of the reasons, discussed above, that the rejections of Claims 1 and 11 should be withdrawn. In addition, while the Office Action cites to Dahlstrom at paragraph 0027 as disclosing the recitations added by Claims 9 and 19, Applicants respectfully submit that the cited passage does not disclose or suggest pruning a TMV to discard at least some of the TMV that is not needed for processing countermeasures. Accordingly, the failure of the cited art to teach this aspect of the invention of Claims 9 and 19 provides an independent basis for withdrawal of the rejections of Claims 9 and 19.

VIII. The Rejections of Claims 10 and 20

Claims 10 and 20 also stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 5). As Claims 10 and 20 depend from Claims 1 and 11, respectively, the rejections of Claims 10 and 20 should be withdrawn for each of the reasons, discussed above, that the rejections of Claims 1 and 11 should be withdrawn. In addition, while the Office Action cites to Dahlstrom at paragraph 0042 as disclosing the recitations added by Claims 10 and 20, Applicants respectfully submit that the cited passage does not disclose or suggest mutating a TMV to a format that is compatible with processing countermeasures as recited in Claims 10 and 20. Accordingly, the failure of the cited art to teach this aspect of the

invention of Claims 10 and 20 provides an independent basis for withdrawal of the rejections of Claims 10 and 20.

X. The Rejections of the Remaining Claims

Claims 5, 8, 15 and 18 likewise stand rejected as obvious over the combination of Flowers and Dahlstrom. (Office Action at 5). The rejections of these claims should be withdrawn at least for each of the reasons, discussed above, that the rejections of the claims from which they depend should be withdrawn.

XI. Conclusion

Applicants submit that the claims are patentable for at least the reasons discussed above. Applicants respectfully request allowance of the claims and passing of the application to issue in due course. Applicants encourage the Examiner to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,

D. Randal Ayers
Registration No. 40,493
Attorney for Applicants

Customer Number 20792
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)